

Heitor Gouvêa

Independent Security Researcher

Alameda Jaú, 150 - Jardins
São Paulo, SP - Brasil

+55 (11) 959 901 602
hi@heitorgouvea.me

SUMMARY

During my work as an Independent Researcher my focus is to help people, organizations and companies take control of their own information. I combine a technical skillset with extensive business experience to help companies understand the threats they face and build intelligent tools to combat risk and future security for both individuals and groups.

In the past I have already found flaws in incredible companies such as: Activision Blizzard, Caixa Econômica Federal, Warren Brazil and others not so famous but equally incredible. And in parallel to this I have also won some awards in the past: first place at Bsidés São Paulo 16th CTF and Hackaflag qualification in 2019 and first place at Campinas Hackathon in 2017.

On my personal website you can see my past public researches: <https://heitorgouvea.me>

EXPERIENCE

Independent Security Researcher

heitorgouvea.me - Self-employed

04/2016 - PRESENT

I work independently and on time as part of research teams to explore cybersecurity vulnerabilities and develop comprehensive strategies to mitigate risks. I have experience with a security researcher and architect. I have already worked as a Red Team Member in incredible security consulting companies like OGASEC, Deloitte Brazil, and CIPHER.

During my independent research, I developed some projects in order to solve some recurring problems or validate a theory discovered and on this page, you can check out some of these currently open source projects:

- [Nipe](#): an engine to make Tor Network your default gateway;
- [Nozaki](#): HTTP fuzzer engine security oriented;
- [Uranus](#): an ecosystem of crawlers for detecting: leaks, sensitive data exposure and attempts exfiltration of data;
- [Spellbook](#): micro-framework for rapid development of security audit workflows;

- Security Advisories: [CVE-2019-15032](#) / [CVE-2019-15033](#) / [CVE-2020-9376](#) / [CVE-2020-9377](#)

LANGUAGES

Portuguese: native proficiency

English: limited work proficiency

TECHNICAL SKILLS

Architecture: high scalability, distributed system, decentralized systems, parallel computing and design patterns;

Client-side: HTML5, CSS3, MaterializeCSS, Sass, JavaScript and AngularJS;

Server-side: Shell Script, PHP, Perl, Python and Mojo Framework;

Database: MongoDB, MySQL/MariaDB and PostgreSQL;

I.T Security: Fuzzing, Vulnerability Research, Pentesting and Red Team Strategies;

Tools: Git, Jekyll, Burp Suite, ida64 and Docker;

Agile Methods: Scrum and Extreme Programming;